AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: /S Bow Bottomly 3/18/2021

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of
(Briefly describe the property to be search
Or identify the person by name and address)
PROPERTY KNOWN AS:
1. A Dell Inspiron laptop computer with service tag HVBQVG1;
2. A Samsung cellular phone with IMEI 355573/03/028571/9;
3. A Motorola cellular phone with MEID A000000E18B8CF

IN POSSESSION OF:
Department of Homeland Security Oklahoma City Office
3625 NW 56th
Oklahoma City, OK

Case No: M-21-172-STE

FILED

2:25 pm, Mar 19, 2021
CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIST. OKLA
By: Andrea Caster, Deputy Clerk

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property *(identify the person or describe property to be searched and give its location)*:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C., §§ 2252A(a)(5)(B)	Possession of child pornography
Title 18, U.S.C. §§ 2252(a)(2)	Distribution of child pornography

The application is based on these facts:

See attached Affidavit of Task Force Officer Melissa Travis-Neal, U.S. Department of Homeland Security, which is incorporated by reference herein.

☒ Continued on the attached sheet(s).

☐ Delayed notice of [No. of Days] days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

Melissa Travis-Neal
Task Force Officer
U.S. Department of Homeland Security

Sworn to before me and signed in my presence.

Date: **Mar 19, 2021**

Judge's signature

City and State: Oklahoma City, Oklahoma

SHON T. ERWIN, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Agent Melissa Travis-Neal being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I have been employed as an Agent with the Oklahoma Attorney General's Office (OAG) since July 2012 and have been a Task Force Officer (TFO) with U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since February 2018, and I am currently assigned to the Office of the Resident Agent in Charge, Oklahoma City, Oklahoma. While employed by OAG and in capacity as a TFO with HSI, I have investigated federal criminal violations related to high technology or cybercrime, and I have gained training and experience investigating child exploitation and child pornography through training from the National Criminal Justice Training Center, Internet Crimes Against Children (ICAC) Task Force, by working with other experienced child exploitation criminal investigators, and by working as the case agent for numerous child exploitation investigations. Additionally, I have observed, reviewed, and identified thousands of child pornography images and videos (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a Deputized Homeland Security Investigations Task Force Officer who is engaged in enforcing criminal laws,

including 18 U.S.C. § 2252 and 2252A, and I am deputized to request and execute search warrants.

2. The statements contained in this affidavit are based in part on information provided by law enforcement officials and others known to me, and on my own experience and background as a law enforcement officer. Since the affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of Title 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) and 2252(a)(2) (distribution of child pornography) have been committed and that the instrumentalities, fruits, and evidence of those crimes will be found in a particular place to be searched.

3. This affidavit is made in support of a search warrant for the following items ("DEVICES"), which are currently in the legal custody of the Department of Homeland Security and located in their secure storage at the Oklahoma City office, 3625 NW 56th Street, Oklahoma City, Oklahoma:

a. a Dell Inspiron laptop computer with service tag HVBQVG1;
b. a Samsung cellular phone with IMEI 355573/03/028571/9; and
c. a Motorola cellular phone with MEID A000000E18B8CF.

I am submitting this affidavit in support of a search warrant authorizing a search of the DEVICES (also described in Attachment A to this affidavit) and the extraction from the DEVICES of electronically stored content and information described in Attachment B

hereto, which content and information constitute instrumentalities, fruits, and evidence of the foregoing violation.

DEFINITIONS

4. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the

visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other

programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

j. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to

access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

k. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

n. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

o. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

p. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND ON WEBSITE A

5. Since at least in or about June 2012, the U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Cyber Crimes Center (C3), Child Exploitation Investigations Unit (CEIU), Victim Identification Program (VIP), as well as various international law enforcement agencies, have been investigating an online website that has been used extensively by persons interested in exchanging images depicting child pornography to meet and become trading partners. This website is referred to as "Website A."

6. Below is a description of how Website A operated since at least in or about June 2012. Website A is a photo (still image) sharing website, hosted outside of the United States. Membership to Website A is free and includes unlimited hosting storage and free photo sharing of digital images (not videos). Website A is organized by different forums according to topic. Examples include forums such as "architecture," "travel," "family," and "autos." Each Website A forum contains albums posted and named by the registered Website A user that created the album.

7. To register for an account, and thus become a "member" of Website A, a user must create a username and provide a valid email address in order to receive a password provided by Website A. Upon receiving this password, the user is prompted to create a new password which will be used to log in to Website A. Once this is done, the user, as a member, may create albums and post images within these albums. A member's albums are listed under his username. A member can create one or more photo albums and has the choice to make an album available to all individuals on the Web (a "public album") or make it a password protected album that is only accessible to individuals who know or have the password. When a member creates an album he may choose to have his contact email address displayed under his username (which appears at the top of the album) to others visiting his albums or instead ask others to "contact via comments." In instances where a member does not display his email address, it is common for the member to post their address in the comment section as a means of contact or when responding to a specific

request from another member. An album contains all of the pictures within that album, along with any posted comments. When a member creates an album he has a choice via a scroll down menu to allow: 1) only Website A members who have created albums to comment; 2) only Website A members to comment (regardless of whether these members have created their own albums on Website A; and 3) anyone accessing Website A (members or non-members) to anonymously comment on the album. Or they may disable the comment feature entirely. Anytime an individual posts a comment to an album, the owner of that album is automatically notified by Website A via the email address they provided. The email message states that a comment was made, and includes the file name of the image commented on, the comment itself, the Website A user name of the person making the comment (if the person posting the comment is a Website A member) and a hyperlinked URL to the image with the corresponding comment. While the member who is the owner of an album cannot directly opt out of receiving these email notifications, if they were to go back into their membership profile and delete the email address they provided they will not receive these automated email notifications.

8. Any individual on the Internet can view and post comments to non-password protected albums ("public albums") on Website A and download the images in those albums. When a Website A member posts a comment to an album that member's username, country flag corresponding to the originating IP address, and the date and time of the comment are displayed next to the comment. When a comment is posted by a non-

member of Website A, portions of the originating IP address and a country flag corresponding to that IP address are displayed next to that comment. Regardless of whether the individual posting a comment is a member or non-member, Website A logs the full originating IP address of the individual posting the comment.

9. Website A has become a popular means for individuals to trade child pornography images, in particular through the "nudity" and "kids" forums. Examples of the names of albums within these two forums are "13 yo boy pics," "street boys," "Cute little brunette," "Baby and Toddler Boys," and "Maria chute chubby 16 yo (nude) (password protected)." Some Website A albums associated with some of the targets of these operations are known to contain child pornography. In these cases, the child pornography is most likely to be in a password protected album, rather than in a public album. While most of the images law enforcement has seen posted in public albums may not constitute child pornography, often evidence from the images, and comments posted about the album (either by other individuals or the member who created the album), indicates that the particular poster or person who created the album has a sexual interest in children and that these individuals' interest in Website A lies in the ability to meet other individuals for the private trading of child pornography. A common scenario is for such a user to post child erotica or preview pictures of children, accompanied by a sexually suggestive title or comment, in a public album as a way to entice or attract other individuals with a sexual interest in children. The poster's purpose is often to solicit comments on the

pictures posted from like-minded individuals. Once these individuals meet on Website A, they then agree to trade Website A passwords, or trade their private child pornography collections elsewhere, often by email, rather than risking trading child pornography on Website A itself. Individuals on the Internet, including Website A users, may regularly monitor public albums on Website A and post provocative comments or images in specific albums related to children with the hope of obtaining the password to other password protected albums or information on individuals that are willing to trade child pornography.

PROBABLE CAUSE

10. In July 2020, a Queensland Police Services (QPS) Detective in Australia identified the following member, "cptmurica7" on Website A.[1] The account profile page provided the following email: cptmurica7@gmail.com, as well as a date when the user became a member: April 4, 2020. Additionally, the account profile page indicated a list of topics in which the member is tagged under; "cptmurica7" has the following tags listed on his profile: "Army, artifact, Blondie, blue, boobs, budding, Chubby, Cousin, drunk, effigy, eyes, friend, girl, guard, hottie, Indian, Lt., married, Milf, national, nude, pfc, Redhead, selfie, sexy, short, Shower, sleepover, Stripper, tanning, wife". The profile page showed member "cptmurica7" had albums with the following names: "Myself 35/male", "Daughters friends mom Kim", "Morgan daughters friend", "Cousins ex wife and her

[1] Website A is a foreign website that is known to me to be used extensively by persons interested in exchanging images depicting child pornography to meet and become trading partners.

daughter", "Daughters friend shower spy", "Army National guard girl", "Cousin", and "Wife."

11. The QPS Detective, working in an undercover capacity, was able to view the contents of "cptmurica7's" albums and capture them in screenshots that were provided to the affiant. The affiant viewed the contents of the albums, provided by QPS via HSI Canberra (Australia). The album titled "Morgan daughters friend" contained pictures of a clothed female, approximately 10-12 years old and closeup pictures of a female's clothed genital region. In an album titled "Daughters friend shower spy", Website A member "cptmurica7" had multiple pictures of a girl, approximately eight to 11 years old; she was getting in or out of the shower, nude and getting dressed. The photos appeared to be taken from a hidden camera inside some sort of zippered container or bag, which was likely sitting on a bathroom vanity. The album titled "Wife" contained multiple pictures of an adult woman with brunette hair, in various stages of undress, nude and performing sexual acts. One of the photos in the "Wife" album depicted the same brunette woman wearing Army fatigues; there was a partial name patch in the photos with the letters "DWIN"

12. On July 2, 2020 at 5:33PM Australian Eastern Standard Time, the QPS Detective, acting in an undercover capacity, emailed cptmurica7@gmail.com. Their correspondence is as follows:

Sent from QPS Detective (undercover) to "Cptmurica7":

Thu, Jul 2, 5:33 PM (all time Australian Eastern Standard Time)

Hey

Saw you [Website A]

I loved your albums, especially Morgan daughters friend

She is hot. Did you get to touch her ass or cunny or drop your cock on her whilst she slept?

Would love to chat as you seem like your into spy stuff like me

alex

Sent from "Cptmurica7" to QPS Detective (undercover)

Thu, Jul 2, 8:19 PM

Thank you for your email. I'm glad that you enjoyed

Sent from QPS Detective (undercover) to "Cptmurica7":

July 2, 2020 - 8:52 PM

Yeah man. Those pics really turned me on

Tell me more cos I love to get off on others doing what I do? :)

alex

July 3, 2020 - 7:42 AM

what happened to you bud. we cool or did i insult you somehow?

Sent from "Cptmurica7" to QPS Detective (undercover)

8:01 AM

We are cool. Just haven't had time to respond

8:02 AM

Email me the link to your [Website A] account for i can view your albums

Sent from QPS Detective (undercover) to "Cptmurica7":

8:15 AM

i dont post on [Website A] anymore. got banned to many times. ive been on there since 2010 & it used to be better back then. you could post anything.

what sort of stuff you into cos im mainly into little girls?

ive got a big collection of all sorts of fetishes cos im a bit of a sick fucker :)

alex

Sent from "Cptmurica7" to QPS Detective (undercover):

8:26 AM

Any females between 10 to 55 mostly 10 to 25 though. Not into any type of professional stuff. I like homemade, spy,voyeur, candid, sister, mom, Aunt cousin.

What's your favorite?

Sent from QPS Detective (undercover) to "Cptmurica7":

8:34 AM

love young girls mainly. 7 - 15 yo. i like new homemade stuff too, but i also like to be active with yung as well whats the spy stuff your postin on your dau's friend? is that original stuff you took or did you get it elsewhere?

10:01 AM

here you go bud. best i could do whilst i am at work

love to get some homemade daughter or her friend pics/vid back

alex

13. On July 14, 2020, HSI Canberra Representative (ICE REP) Phillip Chaves submitted a Department of Homeland Security (DHS) Summons to Google requesting subscriber information for email address cptmurica7@gmail.com. On July 16, 2020, Google responded to the summons with subscriber information. According to Google records, email address cptmurica7@gmail.com was created on April 12, 2020. The name on the account was "Dewayne Baldwin". The recovery email for the Google account was cptmerica7@gmail.com and the recovery SMS was 330/309-0786 [US]. Google provided IP addresses used to access the account including the following IPs:

2600:387:1:805::2c at 2020-07-02 / 10:17:55 UTC

2600:387:1:803::74 at 2020-07-01 / 15:28:44 UTC

2600:1700:8b40:5490:2930:e757:ced6:f552 at 2020-07-04 / 07:01:23 UTC

These IP addresses and phone number were allocated to AT&T.

14. On July 16, 2020, ICE REP Chaves submitted a DHS summons to AT&T for the IP addresses listed above as well as phone number 330/309-0786. The summons requested subscriber information for the specific dates and times outlined above. On July 17, 2020, AT&T responded to the summons and identified the following account holder and address as being the subscriber of the IP address 2600:1700:8b40:5490:2930:e757:ced6:f552: Amber Baldwin, 1718 NW Oak Ave, Lawton, OK 73507, 330/322-5253. On July 19, 2020, AT&T responded to the summons for phone number 330-309-0786 and identified the user as Derek BALDWIN, 5508 Ridge Rd, Cleveland, OH 44129. The phone number was active since July 31, 2010.

15. In August 2020, HSI Oklahoma City received the case from HSI Canberra. On September 7, 2020, I conducted surveillance at 1718 NW Oak Ave in Lawton, Oklahoma. I observed a black Toyota 4Runner and a white, Chevrolet Avalanche parked in the driveway. The Oklahoma license plate for the 4Runner was IXN161. The Avalanche was parked backwards with the license plate facing away from the road and unable to be seen. According to the Oklahoma Tax Commission, the 4Runner was owned by Amber Baldwin. According to the Oklahoma Tax Commission, Derek BALDWIN, was the owner of a 2007 Chevrolet Avalanche with VIN 3GNEC12J77G110680. I conducted surveillance again on December 10, 2020 and January 7, 2021 and observed the same black Toyota 4Runner parked in the driveway.

16. In December 2020, I requested information from the Army Criminal Intelligence Division (CID) for Derek and Amber BALDWIN. According to Army CID Special Agent Tyrone Francis, Derek BALDWIN is an Army National Guard member. BALDWIN'S wife is Amber Baldwin. Amber is Army Active Duty and both are assigned to Fort Sill in Lawton. According to Army records, the Baldwins have one minor child, a daughter who was 10 years old. They reside at 1718 NW Oak Ave, Lawton, Oklahoma 73501 and BALDWIN'S home phone number is (330) 309-0786.

17. I obtained the Oklahoma driver's licenses for both Amber and Derek BALDWIN. Derek Wayne BALDWIN'S license was issued on July 13, 2020 and the address on his driver's license was 1718 NW Oak Ave, Lawton, Oklahoma 73507. Amber Baldwin's driver's license photo looked exactly like the woman in the "Cptmurica7" "Wife" album on Website A.

18. On January 26, 2021, a federal search warrant for 1718 NW Oak Ave, Lawton, Oklahoma was authorized by Gary M. Purcell, U.S. Magistrate Judge. On February 6, 2021, the search warrant was executed at 1718 NW Oak Ave in Lawton, Oklahoma. Derek and Amber BALDWIN and their minor child were contacted at the above address. Numerous electronic storage devices were taken as evidence under the authority of the search warrant.

19. On March 4, 2021, Amber Baldwin contacted this agent via telephone and advised she had found a laptop computer and two cellular phones (the DEVICES)

belonging to and used by Derek BALDWIN in their locked shed outside their house located at 1718 NW Oak Ave in Lawton, Oklahoma. Amber Baldwin offered to give them to me.

20. On March 10, 2021, I retrieved the DEVICES from Amber Baldwin at her home in Lawton with her permission. The items were taken to the HSI Oklahoma City office.

COMPUTERS, THE INTERNET AND CHILD PORNOGRAPHY

21. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera

or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.*, "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Given the storage capabilities, modern computers can retain many years' worth of a user's data, stored indefinitely. Even deleted data can often be forensically recovered. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person or in their immediate vicinity. Digital files can be quickly and easily transferred back and forth between

computers (as broadly defined by 18 U.S.C. § 1030(e)) and other digital file storage devices or stored simultaneously on them. For example, smartphones can often synch with a traditional desktop or laptop computer. This can result in files being transferred from the smartphone to the computer or even stored on both devices simultaneously. Thus, I am requesting to seize and copy all electronic storage media on the DEVICES and search them.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. For example, distributors of child pornography can use membership-based/subscription-based Web sites to conduct business, allowing them to remain relatively anonymous.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can usually be found on the user's computer or external media.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally: the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. Thus, if a user has downloaded image files, viewed them, then deleted them, a computer forensic examiner could oftentimes find evidence of such actions and maybe even the deleted images themselves.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

22. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact

disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate

analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file, which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

23. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices.

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or

interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

24. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

25. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying all computers and electronic storage media on the DEVICES that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

26. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, possess, and/or collect child pornography:

a. Child pornography collectors usually start collecting child pornography by obtaining free images and videos of child pornography widely available on the internet on various locations and then escalate their activity by proactively distributing images they have collected, often for the purposes of trading images of child pornography with others, as a method of adding to their own collection of child pornography.

b. Child pornography collectors may receive sexual gratification,

stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

c. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

d. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years. Collectors prefer not to be without their child pornography for any prolonged time period.

e. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-

based online storage, to enable the collector to view the collection, which is valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

f. Child pornography collectors also may correspond with and/or meet others to share information and materials; keep correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[2]

h. Even if BALDWIN uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence

---

[2] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

of this access will be found in his home, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

i. In light of the aforementioned, including the facts that demonstrate BALDWIN possessed and distributed child pornography, I think (based on my training and experience) that it is highly probable that BALDWIN is a child pornography collector.

27. Based on the evidence in this investigation, I believe that BALDWIN, likely displays characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography.

CONCLUSION

28. Based upon the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the foregoing criminal violations are located in the DEVICES; therefore, I seek a warrant to search the DEVICES for the items listed in Attachment A.

Melissa Travis-Neal
Agent, OK Attorney General's Office
TFO, Homeland Security Investigations

Sworn and subscribed before me this 19th day of March, 2021.

SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

ITEMS TO BE SEARCHED

1. A Dell Inspiron laptop computer with service tag HVBQVG1;

2. a Samsung cellular phone with IMEI 355573/03/028571/9; and

3. a Motorola cellular phone with MEID A000000E18B8CF.

This warrant authorizes the forensic examination of the DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Any and all digital notes, documents, records, or correspondence pertaining to the possession of child pornography as defined in 18 U.S.C. § 2256(8).

2. Any and all digital images of child pornography as defined in 18 U.S.C. § 2256(8).

3. Any and all digital notes, documents, records, or correspondence identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8).

4. Any and all digital notes, documents, records, or correspondence concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8).

5. Any and all digital notes, documents, records, or correspondence concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography.

6. Any and all digital notes, documents, records, or correspondence concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

7. Any and all digital records, documents, invoices and materials that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection

to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Any and all digital address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8).

9. Any and all records tending to identify the owner or user of the DEVICES described in the affidavit.

10. Any and all diaries, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

11. Any and all records pertaining to how the user of the DEVICES acquired or disseminated any child pornography.

12. Any and all records pertaining to a sexual interest in children.

13. Any federal law enforcement officer may perform or assist with the search for the aforementioned items, including representatives of the United States Attorney's Office.